RASH MADRID

Nº 40

RED & ANARCHIST SKINHEADS SECCIÓN MADRID

http://www.nodo50.org/rashmadrid rashmadrid@nodo50.org

Oct. 10

¿CONTRASEÑAS SEGURAS?

Hoy en día es raro no tener que estar recordando una o más contraseñas. Estas están presentes en nuestras vidas queramos o no. Las podemos encontrar en nuestra dirección de correo electrónico, foros, webs, redes sociales, tarjetas de crédito, alarmas, el DNI electrónico, etc.

Partiendo de la base de que es difícil "escapar" de ellas lo que debemos de tener muy presente es la seguridad que tienen nuestras contraseñas y si estas se están repitiendo en varios servicios a la vez.

Como hacer que una contraseña sea segura.

Lo primero para tener una contraseña segura aunque parezca una tontería es que esta nunca sea similar a la de otro servicio. Por poner un ejemplo si nosotros nos vamos a registrar en la red social Tuenti y usamos nuestro correo electrónico habitual nunca deberemos poner en esta red social la misma contraseña que la que tenemos en nuestro correo electrónico.

Parece algo obvio pero es un fallo muy común y a los hechos me remito. Recientemente la empresa de seguridad informática BitDefender ha realizado un estudio en el que nos dice que 3 de cada 4 internautas es decir el 75% es asiduo a utilizar la misma contraseña en el correo electrónico que en la red social, principalmente ocurriendo esto en Tuenti y Facebook.

Teniendo el concepto claro de que no debemos repetir contraseñas lo siguiente que debemos hacer es crear una contraseña fuerte y robusta. Para ello lo mejor es hacer una combinación de números, letras mayúsculas, letras minúsculas y símbolos (& % $! = ? *· – /). A la hora de crear la contraseña excluiremos nombres de familiares, amigos o cualquier palabra que tenga relación contigo.

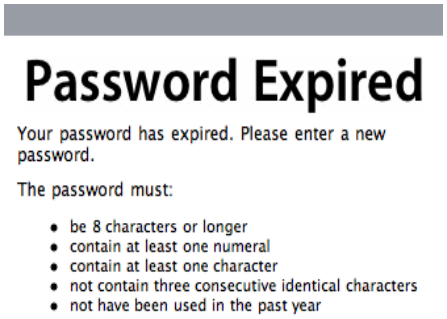
Por ejemplo vamos a utilizar la palabra electronic y vamos a convertirla en una contraseña más o menos segura. Sustituiremos primeramente las vocales por números, es decir, si tenemos (a,e,i,o,u) sustituimos por (4,3,1,0,>), después añadimos algún carácter extraño y metemos alguna mayúscula entre medias. Un ejemplo final de esto podría ser El3t%r0N1c.

Ahora bien tenemos una contraseña segura pero como veis esta es bastante difícil de recordar y más aun si tenemos que recordar varias contraseñas creadas de la misma manera. Como solución os sugiero usar el programa Keepass (**http://keepass.info**) que tiene versiones para diferentes sistemas operativos y es bastante fácil de usar. Este programa nos permitirá almacenar todas nuestras contraseñas y guardar estas bajo una clave maestra entre otros métodos de seguridad. Por lo tanto al fin y al cabo con que nos sepamos solo una de las contraseñas de memoria nos servirá.

El siguiente aspecto a tener en cuenta es no caer en ataques de phishing, que para que todos lo entendamos es la suplantación de una página web, es decir, te hacen creer que estas accediendo a http://www.hotmail.es pero en realidad estas en http://www.hotmail.tk por poner algún ejemplo. Esto suele pasar porque la gente suele confiar del contenido de correos electrónicos o bien porque han sido infectados por un "virus". Para evitarlo fíjate siempre en la url en la que estas antes de ingresar en algún momento tu nombre de usuario y contraseña de cualquier sitio. A

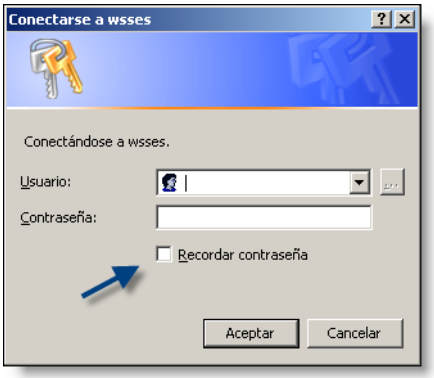
modo de curiosidad este método es sobre todo bastante utilizado en la banca electrónica suplantando por ejemplo páginas como la de Caja Madrid.

De hecho hace cuestión de un año aproximadamente se produjo un ataque de phising en hotmail,gmail y yahoo en el cual se consiguió la contraseña de más de 30000 cuentas de correo. Estas cuentas de correo con sus respectivas contraseñas fueran difundidas por internet lo cual destapó que las contraseñas más utilizadas solían ser cosas como password, 123456, 123456789, qwerty, abc123, o incluso el propio nombre del usuario.



Otra cosa bastante importante es el cambio de las contraseñas periódicamente siendo lo más recomendable entre 3 o 6 meses, de hecho ciertos servicios te dan la posibilidad de que tu contraseña caduque cada X tiempo y te recuerdan cada ese tiempo cambiarla. Sin embargo podréis pensar que es bastante engorroso que una vez que te has aprendido esa contraseña tan difícil tengas que volver a cambiarla, pero imagina que has sido infectado por algún virus en tu ordenador o bien alguien ha descubierto tu contraseña pero no ha dejado un rastro de ello. El tendrá tu contraseña hasta que él quiera pero si tú la cambias cada x tiempo llegará un momento en que se le corte el rollo.

Otro error bastante común es la utilización del típico servicio de recordar contraseña que nos ofrecen los navegadores web como pueden ser Firefox, Chrome, etc. A pesar de que en nuestro ordenador tengamos una cuenta de usuario cerrada a cal y canto imagina que un día por alguna razón olvidaste cerrar tu sesión y por tanto acceder a tu navegador es cuestión de un click de ratón y por ejemplo en Firefox sería tan simple como ir a Herramientas, Seguridad y a Contraseñas guardadas y luego darle a Mostrar contraseñas y estaríamos dejando al descubierto todas las contraseñas que hayamos guardado. Y no solo ocurre esto en los navegadores sino también en los clientes de correo como Outlook o Thunderbird y también deberemos tener precaución con esto.



Un factor también importante es el de la pregunta secreta la cual nos aparece en registros en ciertas webs, foros e incluso para crear cuentas de correo electrónico (GMail, Hotmail, Yahoo, AOL, etc.).

Esta pregunta secreta normalmente viene preestablecida, es decir, te dan a elegir entre unas cuantas preguntas y tu elijes la que veas más adecuada para luego posteriormente si surgiera algún problema poder recuperar nuestra cuenta. Sin embargo esta pregunta puede a veces suponer más un riesgo que una seguridad para nuestra cuenta si no la utilizamos de forma correcta.

La mejor forma de utilizarla es dando respuestas absurdas a cualquiera de las preguntas predefinidas. Por ejemplo si elegimos una pregunta del tipo: ¿Como se llama tu mascota? responderemos algo como por ejemplo Llueve en Madrid pero hace calor en Barcelona. Si, no tiene sentido, pero si hubiéramos contestado algo verdadero sería cuestión de tiempo descubrirlo.

Haciendo un resumen rápido las claves básicas para tener una contraseña segura es:

-No repetir la contraseña en diferentes servicios.

-La contraseña debe contener una combinación de números letras y símbolos.

-Fijarse en que no nos estén haciendo caer en un ataque de phishing.

-Cambiar la contraseña de forma periódica.

-No usar servicios de recordar contraseñas.

-Responder cosas absurdas frente a las preguntas secretas de ciertos servicios.

A pesar de todas estas medidas una contraseña nunca será completamente segura pero al menos basándonos en estos conocimientos será mucho más difícil el que está esté expuesta a que alguien nos la pueda adivinar o consiga quitárnosla.